AF/S

Docket No.: 826.1722

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re the Application of:

Naoya FUJISAKI

Serial No. 09/819,701 Group Art Unit: 2161

Confirmation No. 3142

Filed: March 29, 2001 Examiner: E. LEROUX

For: FILE SYSTEM ASSIGNING A SPECIFIC ATTRIBUTE TO A FILE, A FILE MANAGEMENT METHOD ASSIGNING A SPECIFIC ATTRIBUTE TO A FILE, AND A STORAGE MEDIUM ON WHICH IS RECORDED A PROGRAM FOR MANAGING FILES

APPEAL BRIEF

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

I. Real Party in Interest

The inventor, Naoya Fujisaki, assigned all rights in the subject application to FUJITSU LIMITED on March 9, 2001 according to the Assignment executed March 9, 2001 which was submitted for recordation on March 29, 2001 and recorded at Reel 11653, Frames 922-923. Therefore, the real party in interest is FUJITSU LIMITED.

II. Related Appeals and Interferences

There are no related appeals or interferences known to Appellants, Appellants' legal representatives or the Assignee, FUJITSU LIMITED, which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. Status of Claims

Claims 1-18 are pending in the application. In the paragraph numbered "1" on page 2 of the final Office Action dated January 20, 2006, it was stated that claims 1-8, 15, 16 and 18 were rejected under 35 U.S.C. § 102(e) and in the second paragraph on page 4 of the January 20,

2006 Office Action, it was stated that claims 11-14 and 17 were rejected under 35 U.S.C. § 103(a). As noted in the Amendment filed by certificate of mailing on November 14, 2005 (received by the U.S. Patent and Trademark Office on November 16, 2005), the status of claims 9 and 10 was not indicated in either the January 20, 2006 Office Action, or the August 11, 2005 Office Action. From the discussion following the statements setting forth the rejections, it appears that the Examiner intended to reject claims 1-6, 9 and 10 under 35 U.S.C. § 102(e) and claims 7, 8, 11-14 and 17 under 35 U.S.C. § 103(a).

For purposes of appeal, it will be assumed that claims 1-6, 9, 10, 15, 16 and 18 stand rejected under 35 USC § 102(e) and claims 7, 8, 11-14 and 17 stand rejected under 35 USC § 103(a).

IV. Status of Amendments

The Amendment filed by certificate of mailing on November 14, 2005 (received by the U.S. Patent and Trademark Office (USPTO, hereafter) on November 16, 2005) in response to the August 11, 2005 Office Action presumably was entered by the January 20, 2006 Office Action. No Amendment was filed in response to the January 20, 2006 Office Action.

V. Summary of Claimed Subject Matter

The application is directed to managing files in a computer system (page 1, lines 14-24) by assigning policy attribute data to a directory or to a subdirectory, such as by inheritance (page 11, lines 1-15). For example, by setting a specific volume number in a directory as policy attribute data, the manager of a file system can designate the storing place of a file (page 11, lines 18-22). Thus, a file that is accessed often can be stored on a disk having a high access speed and the access time of the file can be reduced accordingly (page 6, lines 9-11). As another example, by setting the constraints of disk capacity as the policy attribute data of a directory, the disk capacity of a file within a specific directory can also be limited (page 11, line 23 to page 12, line 1). Thus, control and statistical information of disk capacity to be used by a file (page 12, lines 4-10) and the total size of files within a directory can be managed (page 12, lines 19-22). When a file is archived, preferably the policy attribute data is stored in a hidden file, so that when the file is restored, the hidden file can be read by the operating system and used to control how the file is restored (page 13, line 3 to page 14, line 9).

Claims 1 and 2 recite a "computer system for managing a file on at least one volume" for example, as discussed in the first two paragraphs of the application. The first element recited in claims 1 and 2 is "a setting unit" (line 2) which is defined at page 8, lines 6-10 as part of the file

system. Page 18, lines 11-12 refers to "a program implementing the policy control module 2" illustrated in Figs. 5 and 13 and which is thus embodied by a processor programmed to perform the operations described, e.g., at page 18, line 11 to page 19, line 25 with reference to the flowchart in Fig. 3.

The setting unit recited in claims 1 and 2 sets "policy attribute data specifying file usage, determined by an administrative user, in correspondence with path information of a directory" (lines 2-3). As described in the specification, an "administrator of the file system 1 registers policy data to be processed" (page 18, lines 16-17, and Fig. 3, block 11). "The policy data registered at this time is structured by the path information of a directory" (page 18, lines 18-19). The specification contains several examples of policy attribute data that can be specified by an administrative user. One is that, "a file system administrator can specify the storage location of the file" (page 6, lines 7-9) which relates to "path information".

While the term "file usage" does not appear in the application as filed, the term "file operation" is used at page 7, line 15; page 15, line 12; page 31, last line; and page 39, lines 19-20 and the word "operation" is used elsewhere in the specification in reference to files. In addition, there are specific examples of "file usage" or "file operations" such as "a move of the file data within the Y directory from the volume allocation 'volume-ID=1' to 'volume-ID=2'" (page 32, lines 13-15) and other operations that affect "quota" where "quota is defined as one piece of attribute data possessed by policy data, whereby an administrator of the file system 1 can restrict the disk capacity used for files within a directory" (page 30, line 23 to page 31, line 2).

Claim 1 also recites "a file managing unit managing a file based on policy data composed of the path information of the directory and the policy attribute data" (claim 1, last 2 lines). The term "file managing unit" (page 5, line 21) is embodied by a "file management program" (page 36, line 24) that is "executed by being loaded into a user computer" (page 36, line 22) for "implementing the above described file system" (page 36, line 19) and thus, corresponds to a programmed processor. An example of what "the above described file system" does is when "the policy control module 2 checks the attribute data of the target file and the directory at the move destination (step S21 of Fig. 13)" (page 33, lines 22-24).

Claim 2 also recites "an assigning unit assigning policy attribute data of a directory so as to be inherited to a subdirectory, or assigning specified policy attribute data indicating a policy on which file management is based to the subdirectory" (claim 2, last 3 lines). The assigning unit recited in claim 2 is described at page 8, lines 10-15 and page 9, lines 1-8, . Examples are provided at page 9, lines 12-15 and page 11, lines 4-15.

Claim 15, recites a "file management method for use in a file system configured by one or a plurality of volumes" (claim 15, lines 1-2) in which operations are performed that include those described above as being performed by the policy control module 2 (page 18, lines 11-12; page 33, lines 22-24; Figs. 5 and 13). The operation of "managing a file based on policy data composed of the path information of the directory and the policy attribute data" (claim 15, last 2 lines) is the same operation performed by the "file managing unit" recited on the last 2 lines of claim 1. The operation of "setting policy attribute data" on lines 3-4 of claim 15 differs from the operation performed by the "setting unit" recited on lines 2-3 of claim 1 in that the "policy attribute data [are] indicating a policy ... on which file management is based" (claim 15, lines 3-4) rather than "specifying file usage" (claim 1, line 2) and thus, claim 15 is broader since file "management" may not involve "usage." There are many examples of file management in the specification several of which are described on pages 6-8.

Claim 16 recites a "computer-readable storage medium on which is recorded a program for causing a computer to execute a process" (claim 16, lines 1-2) in which the same operations recited in claim 15 are performed. Thus, the analysis provided above for claim 15 applies to claim 16.

Claim 17 recites a "computer-readable storage medium on which is recorded a program for causing a computer to execute a process" (claim 17, lines 1-2). As in claims 15 and 16, the first operation performed in the process recited in claim 17 involves "setting policy attribute data indicating a policy on which file management is based, in correspondence with path information of a directory" (claim 17, lines 3-4). However, claim 17 adds that the policy is also set "in correspondence with ... file usage specified by an administrative user" (claim 17, lines 4-5). Thus, the "policy data" in claim 17 includes aspects of the policy data that is set in claim 1 as well as in claims 15 and 16.

Next, claim 17 recites "assigning ... policy attribute data for files in the directory to be inherited to a subdirectory" (claim 17, lines 6-7), as described at page 8, lines 10-15 and page 9, lines 1-8. Examples are provided at page 9, lines 12-15 and page 11, lines 4-15.

Finally, claim 17 recites "assigning specified policy attribute data for files in the subdirectory to a corresponding subdirectory when moving the directory" (claim 17, last 2 lines), as described at page 8, lines 16-18. An example is provided at page 9, lines 15-19.

Claim 18 recites a "file management method for a file system having at least one volume" (claim 18, line 1) in which the first operation performed is "setting policy attribute data indicating

a policy, determined by an administrative user, for storing a file depending on type of information in the file, file usage specified by an administrative user and path information of a directory in which the file is stored" (claim 18, lines 2-4). The only item that claim 18 recites the storing as "depending on" that was not discussed with respect to claims 15 and 16 is "type of information in the file" (claim 18, line 3). As described at page 2, lines 7-9, "a policy for distributing information to disk devices depending on the type of information ... [may be] introduced."

Next, claim 18 recites "managing the file based on policy data composed of the path information of the directory and the policy attribute data" (claim 18, last 2 lines), as described in the last paragraph on page 5 of the application. The term "policy data" is defined in the sentence spanning pages 7 and 8 as "path information of a directory and policy attribute data" and is illustrated in Fig. 1 which is described at page 18, lines 18-23.

VI. Issues to be Reviewed on Appeal

Assuming that claims 9 and 10 in addition to claims 1-6 (but not claims 7and 8, as stated in the January 20, 2006 Office Action) were rejected under 35 U.S.C. § 102(e) and claims 7, 8, 11-14 and 17 were rejected under 35 U.S.C. § 103(a), at issue is (1) whether U.S. Patent 5,437,029 to Sinha discloses all of the limitations recited in claims 1-6, 9, 10, 15, 16 and 18; (2) whether Sinha teaches or suggests all of the limitations recited in claims 7, 8 and 17 and the claims from which claims 7 and 8 depend; (3) whether the combination of Sinha and U.S. Patent 5,832,527 to Kawaguchi teaches or suggests all of the limitations recited in claim 11 and claim 1 from which it depends; (4) whether the combination of Sinha and U.S. Patent 6,185,574 to Howard et al. teaches or suggests all of the limitations recited in claim 12 and claim 1 from which it depends; (5) whether the combination of Sinha, Howard et al. and U.S. Patent 6,195,695 to Cheston et al. teaches or suggests all of the limitations recited in claims 13 and 14 and the claims from which they depend; and (6) whether the combination of Kawaguchi and U.S. Patent 6,018,741 to Howland et al. teaches or suggests all of the limitations recited in claim 17.

VII. Argument

As discussed above, it will be assumed that the January 20, 2006 Office Action rejected claims 1-6, 9, 10, 15, 16 and 18 (but not claims 7 and 8) under 35 U.S.C. § 102(e) as anticipated by Sinha.

Rejections under 35 USC § 102(e)

In rejecting claim 1, the Examiner cited the Abstract and portions of columns 1, 2 and 8. As discussed in the Amendment received by the USPTO on November 16, 2005, the cited portions of columns 1 and 2 in Sinha describe Figs. 1 and 2 which show that when a file c 83 (Fig. 1) is to be accessed, node 1 (Fig. 2) searches its root directory to find that directory a is in node 2. Conventionally, node 2 finds that directory b is in node 3 which finds file c in directory b. Thus, node 1 accesses directory b in node 3 to obtain the location of file c, so that it can access the data therein. In Sinha, location data about directories a and b and file c is stored in the cache of each node. As a result, node 1 can access file c in the directory b of node 3 without accessing node 2.

The cited portion of column 8 in Sinha describes that a file entry is "deleted from the SPNT cache" (column 8, line 38) when "a sufficient number of users ... in succession" (column 8, lines 36-37) access "the file while specifying a path name resolution mode which does not utilize the SPNT cache" (column 8, lines 32-34) which causes the "reference counter value for the corresponding file entry within the SPNT cache ... [to be] decremented" (column 8, lines 34-36). When the reference counter value reaches zero, the file entry is deleted, as described in the Abstract.

As discussed in the Amendment received by the USPTO on November 16, 2005, nothing has been found in the cited portions of Sinha regarding anything "determined by an administrative user" (claim 1, lines 4-5), as recited in all of the independent claims. Nor was anything found in Sinha regarding any "attribute data specifying file usage" (claim 1, line 3), other than a counter that indicates how the file is being accessed. The other information about files in the cited portions of Sinha relate to location, not usage. Furthermore, no occurrence of any form of the word "administrate" has been found in Sinha. As claims 1, 15, 16 and 18 all recite "setting policy attribute data ... determined by an administrative user" (e.g., claim 1, lines 4-5), claims 1, 15, 16 and 18, as well as claims 2-6, 9 and 10 which depend from claim 1, patentably distinguish over Sinha.

In response to the arguments above that were presented in the Amendment received by the USPTO on November 16, 2005, on pages 9 and 10 of the Response to Arguments, the Examiner suggested that the term "administrative user" could be interpreted as a "system administrator" who has five typical duties listed on page 9 of the January 20, 2006 Office Action. While this is a possible definition of the term "administrative user," the Examiner then proceeded to assert that the "user of a system [who] can specify that a particular file, located at

some other system in the network, is to be accessed using a local search mode of path name resolution, providing high access performance with fixed access speed" (Sinha, Abstract, lines 3-7) is a "System Administrator who allocates mass storage space" (January 20, 2006 Office Action, page 11, line 2).

It is submitted that the Examiner has misinterpreted the term "user" in the Abstract of Sinha, by reading the Abstract in light of the claimed invention, instead of trying to determine what one of ordinary skill in the art would learn from Sinha taken as a whole. First, it is noted that the Abstract states, "**each** user of a system can specify" (Sinha, Abstract, lines 2-3, emphasis added) how the file is to be accessed. It is submitted that it would be a very unusual system in which "each user" is a System Administrator.

Second, included in the quotation of the entire Abstract of Sinha at the bottom of page 10 in the January 20, 2006 Office Action is the statement that "the directories of the path name of that file which are resident in other systems of the network are then replicated on disk at the user's system" (Sinha, Abstract, lines 7-9) which implies that the "user" in the sentence on lines 1-7 of Sinha's Abstract is not responsible for a whole networked system as is typical of a System Administrator, but rather a user of a single node, such as the "user of node 1 [who] requires to access the file c" (Sinha, column 1, lines 60-61) where, as explained at column 1, lines 54-59, node 1 of the user is represented by the circle with reference numeral 80 in Fig. 1 and file c is represented by the box associated with reference numeral 83.

Third, the word "user" also appears in the final sentence in the Abstract of Sinha which starts with "[e]ach subsequent request by a user of that system ... results in each of the counters being incremented by 1" (Sinha, Abstract, lines 11-14). Like the first sentence of the Abstract, this implies that "each user" at a node is treated equally. The only difference between the user in the first sentence of the Abstract and the user in the last sentence of the Abstract is that the first sentence describes what happens the first time a file is accessed. Nothing was cited or found anywhere in Sinha to suggest that any "user" mentioned in the Abstract or elsewhere in Sinha has greater authority than any other user and thus would qualify as a "System Administrator" as defined by the Examiner, or an "administrative user" as that term is used in the claims of this application. When the Abstract of Sinha is read in light of the rest of Sinha, it is clear that the sentence on lines 1-7 in the Abstract of Sinha refers to a non-administrative user specifying how a file that is needed at a node is to be accessed and that none of the "typical duties" of a system administrator are being performed.

The Response to Arguments of the January 20, 2006 Office Action in the third paragraph on page 11, asserted that column 8, lines 25-40 of Sinha discloses "file usage data, i.e., file accessing speed based on file usage" (page 11, lines 8-9). This portion of Sinha states "each user of the distributed system can specify, for accessing any particular file, whether or not maximum accessing speed (using the SPNT cache) will be required, whenever the file is accessed in future" (Sinha, column 8, lines 25-28). It is submitted that there is nothing in this statement indicating that the speed is "based on file usage." There is no suggestion in column 8, lines 25-40 of Sinha of "policy attribute data specifying file usage" (claim 1, line 2), i.e., **how** a file is used, only whether it is cached. It is submitted that this does not constitute "file usage" by any definition.

As mentioned in the Summary of Claimed Subject Matter, the term "file usage" is not used in the specification, but the term "file operation" is and there are examples of file operations on pages 30-32, for example, which it is it submitted qualify as "file usage." However, it is submitted that specifying storage of a file in cache to increase speed of access, as taught by Sinha, does not constitute "file usage" as that term is used in the claims.

It is submitted that independent claims 1, 2, 15, 16 and 18, all of which recite operations performed by "an administrative user" (claim 1, lines 2-3; claims 15 and 16, line 3; and claim 18, line 2) are not anticipated by Sinha. Furthermore, claims 1, 2 and 18 which also recite "file usage" and claims 3-6, 9 and 10 which depend from claim 1, patentably distinguish over Sinha for all of the above reasons.

As discussed at page 7, lines 8-10 of the Amendment received by the USPTO on November 16, 2005, no form of the word "inherit" or any synonymous term has been cited or found in Sinha. Since there was no rebuttal of this argument in the "Response to Arguments" on pages 9-12 of the January 20, 2006 Office Action, it is submitted that claim 2 further patentably distinguishes over the prior art due to the failure of Sinha to teach or suggest "assigning policy attribute data of a directory so as to be inherited to a subdirectory" (claim 2, lines 4-5).

Rejections under 35 USC § 103(a)

On pages 4-5 of the Office Action, claim 7, 8 and 17 were rejected under 35 USC § 103(a) as unpatentable over Sinha. Claims 7 and 8 depend from claim 2 and therefore, it is submitted that claims 7 and 8 patentably distinguish over Sinha for all the reasons set forth above with respect to claim 2.

In rejecting claim 7, it was acknowledged that Sinha "fails to disclose ... [that] policy attribute data of a parent directory is inherited to a subdirectory ..." (January 20, 2006 Office Action, page 4, lines 11-13). However, the January 20, 2006 Office Action asserted that the disclosure of prior art "root directory and a subdirectory which may be a child or grandchild of the rood directory" (January 20, 2006 Office Action, page 4, lines 15-16) was sufficient to make it obvious to one of ordinary skill in the art to perform the operations recited in claim 7. The only reason given in support of this assertion of obviousness was "for the purpose of quickly locating a file by successively searching a path from a root directory to subdirectories" (January 20, 2006 Office Action, page 4, lines 21-22).

It is submitted that the reason given by the Examiner in support of finding that claim 7 is obvious is insufficient to support the rejection and does not overcome the deficiencies of Sinha discussed above with respect to claim 2. The operations recited in claim 7 are not related to "successively searching a path" but rather define what "policy attribute data" are assigned to files in a subdirectory. Claim 7 does not relate to finding a file in a subdirectory, but rather determining the specifications of "file usage" that apply to the files in a subdirectory. Therefore, it is submitted that claim 7 further patentably distinguishes over Sinha.

In rejecting claim 8, it was acknowledged that Sinha "is silent regarding whether or not to require inheritance is predefined for the policy attribute data" (January 20, 2006 Office Action, page 4, last 2 lines) as well as the remainder of the limitations recited in claim 8. However, it was asserted that it would have been obvious to modify Sinha to meet these limitations "for the purpose of creating a policy that enables files to be quickly accessed considering that files could be distributed throughout a network" (January 20, 2006 Office Action, page 5, lines 12-13). As in the case of claim 7, the reason for modifying Sinha to allegedly make claim 8 obvious seems to have nothing to do with the limitations recited in claim 8.

As discussed above with respect to claim 2 from which claim 8 depends, nothing has been cited or found in Sinha regarding the concept of "inheritance ... for ... policy attribute data" (claim 8, line 2). Unlike Sinha, claim 8 is not related to enabling "files to be quickly accessed" (January 20, 2006 Office Action, page 5, line 12), but rather determining the specifications of "file usage" that apply to the files in a subdirectory. There is nothing in the January 20, 2006 Office Action which explains why controlling whether and how long a file is cached as taught by Sinha has anything to do with whether or not a subdirectory inherits policy attribute data from a parent directory. Therefore, it is submitted that claim 8 further patentably distinguishes over Sinha.

On pages 5-6 of the January 20, 2006 Office Action, claim 11 was rejected under 35 USC § 103(a) as unpatentable over Sinha in view of Kawaguchi for the same reasons as in the August 11, 2005 Office Action. In the paragraph spanning pages 11-12 in the Response to the Arguments to the Amendment received by the USPTO on November 16, 2005, the Examiner addressed the arguments responding to this rejection by noting that "one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references" (January 20, 2006 Office Action, page 11, lines 17-18). This statement has nothing to do with the arguments made in the Amendment received by the USPTO on November 16, 2005 which related to the change in prior art used to reject the independent claims from the Office Action mailed April 23, 2004.

As stated at page 7, lines 16-18 of the Amendment received by the USPTO on November 16, 2005, "Kawaguchi fails to disclose a policy set by an administrative user as recited in the independent claims ... [and as] discussed above, Sinha also fails to teach this feature of the present invention." While the lack of disclosure was discussed with respect to each reference, it was the same feature that is missing from each reference. Nothing was cited or found in either reference regarding an "administrative user" and as a result, the combination of these patents fails to teach or suggest anything that such a user might do. Therefore, as stated in the Amendment received by the USPTO on November 16, 2005, it is submitted that claim 11, patentably distinguishes over the combination of Sinha and Kawaguchi for the reasons discussed above with respect to claim 1 from which claim 11 depends.

On page 6 of the January 20, 2006 Office Action, claim 12 was rejected under 35 USC § 103(a) as unpatentable over Sinha in view of Howard et al. and on pages 7 and 8 of the Office Action, and claims 13 and 14 were rejected under 35 USC § 103(a) as unpatentable over Sinha in view of Howard et al. and further in view of Cheston et al. As discussed in the Amendment received by the USPTO on November 16, 2005, nothing was cited or has been found in Howard et al. or Cheston et al. suggesting modification of Sinha to overcome the deficiencies discussed above. As claim 12 depends from claim 1 and claims 13 and 14 depend from claim 1 via claim 12, it is submitted that claims 12-14 patentably distinguishes over Sinha in view of Howard et al. with or without Cheston et al. for at least the reasons discussed above with respect to claim 1.

In response to the argument that Howard et al. and Cheston et al. fail to suggest modification of Sinha to overcome the deficiencies discussed with respect to claim 1, the Response to Arguments in the January 20, 2006 Office Action again noted that "one cannot show nonobviousness by attacking references individually where the rejections are based on

combinations of references" (January 20, 2006 Office Action, page 12, lines 8-9). Apparently the Examiner cannot recognize an argument that discusses a combination of references. As stated in *In re Lee*, 277 F3d 1338, 61 USPQ2d 1430 (Fed. Cir. 2002),

> the examiner can satisfy the burden of showing obviousness of the combination "only by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the references"

(61 USPQ2d at 1434, citing *In re Fritch*, 972 F.2d 1260, 1265, 23 USPQ2d 1780, 1783 (Fed. Cir. 1992)). The failure of the August 11, 2005 and January 20, 2006 Office Actions to cite anything in Howard et al. and Cheston et al. that would suggest modification of Sinha to overcome the deficiencies thereof discussed in the Amendment received by the USPTO on November 16, 2005 means that the **combination** of these references cannot teach or suggest the invention and there is no motivation to combine these references to meet the limitations that Sinha does not teach or suggest. Therefore, it is submitted that claim 1, as well as claim 12 which depends therefrom, patentably distinguish over the combination of Sinha in view of Howard et al. and claim 1, as well as claims 13 and 14 which depend therefrom, patentably distinguish over Sinha in view of Howard et al. and further in view of Cheston et al. for the reasons that claim 1 patentably distinguishes over Sinha when taken alone, because Sinha, Howard et al. and Cheston et al. when taken in combination contain no suggestion of the features that cannot be found in Sinha.

On page 8 of the January 20, 2006 Office Action, claim 17 was rejected as unpatentable over Kawaguchi in view of Howland et al. As noted in the Amendment received by the USPTO on November 16, 2005, claim 17 was amended by the Amendment filed June 21, 2005 to include a limitation similar to that recited in the other independent claims regarding "file usage specified by an administrative user" (claim 17, lines 4-5). The January 20, 2006 Office Action, like the August 11, 2005 Office Action, failed to identify where either Kawaguchi or Howland et al. or the combination thereof discloses an administrative user specifying file usage. Therefore, it is submitted that claim 17 patentably distinguishes over Kawaguchi in view of Howland et al. for the reasons set forth in the June 21, 2005 Amendment.

Summary of Arguments

For the reasons set forth above and in the Amendment received by the USPTO on November 16, 2005, it is submitted that claims 1-18 patentably distinguish over Sinha, Howard et al., Kawaguchi, Cheston et al. and Howland et al., taken individually or in combination. Thus, it is respectfully submitted that the Examiner's final rejection of the claims is without support and,

therefore, erroneous. Accordingly, the Board of Patent Appeals and Interferences is respectfully urged to so find and to reverse the Examiner's final rejection.

Please charge any required fee to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 8/11/06

By: Richard A. Gollhofer
Richard A. Gollhofer
Registration No. 31,106

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

VIII. Claims Appendix

1. A computer system for managing a file on at least one volume, comprising:

a setting unit setting policy attribute data specifying file usage, determined by an administrative user, in correspondence with path information of a directory; and

a file managing unit managing a file based on policy data composed of the path information of the directory and the policy attribute data.

2. A computer system for managing a file on at least one volume, comprising:

a setting unit setting policy attribute data specifying file usage, determined by an administrative user, in correspondence with path information of a directory; and

an assigning unit assigning policy attribute data of a directory so as to be inherited to a subdirectory, or assigning specified policy attribute data indicating a policy on which file management is based to the subdirectory.

3. The file system according to claim 1, wherein information indicating whether or not to require a path search is registered in correspondence with the policy attribute data.

4. The file system according to claim 3, further comprising a control table storing information indicating a directory to be searched next, wherein pointer information pointing to a storage location within said control table is registered as policy attribute data of a directory.

5. The file system according to claim 4, wherein checkpoint information indicating path information of a directory yet to be generated is registered to said control table for the directory.

6. The file system according to claim 4, wherein checkpoint information registered to said control table is searched, and a directory for which the checkpoint information is set is searched.

7. The file system according to claim 2, wherein when a name of a directory is changed, policy attribute data of a parent directory is inherited to a subdirectory if policy attribute data is not specified for the subdirectory, and specified policy attribute data is assigned to a subdirectory if the policy attribute data is specified for the subdirectory.

8. The file system according to claim 2, wherein:

whether or not to require inheritance is predefined for the policy attribute data; and

policy attribute data of a parent directory is assigned so as to be inherited to a subdirectory if the policy attribute data of the parent directory is data which is requested to be inherited, or specified policy attribute data is assigned to the subdirectory if the policy attribute data of the parent directory is data which is not requested to be inherited.

9. The file system according to claim 1, further comprising a policy violation registering unit registering policy violation information indicating a policy attribute violation to corresponding policy attribute data, if a file operation which violates the policy attribute data is performed.

10. The file system according to claim 1, further comprising a policy recovering unit causing a file or a directory which violates a policy to comply with the policy, and deleting corresponding policy violation information.

11. The file system according to claim 1, wherein information of a total size of files within a directory is registered as policy attribute data of the directory.

12. The file system according to claim 1, wherein when a file is stored in an archive file, policy data composed of path information of a directory and policy attribute data is stored in the archive file.

13. The file system according to claim 12, further comprising a registering unit reading and registering the policy data stored as a hidden file in the archive file, when the file is backed up.

14. The file system according to claim 13, wherein when a file is restored, a comparison is made between path information of a directory to be generated and path information of a directory within the policy data stored as the hidden file in the archive file, and the policy attribute data is set for the directory the path information of which matches.

15. A file management method for use in a file system configured by one or a plurality of volumes, comprising:

setting policy attribute data indicating a policy, determined by an administrative user, on which file management is based in correspondence with path information of a directory; and

managing a file based on policy data composed of the path information of the directory and the policy attribute data.

16. A computer-readable storage medium on which is recorded a program for causing a computer to execute a process, said process comprising:

setting policy attribute data indicating a policy, determined by an administrative user, on which file management is based in correspondence with path information of a directory; and

managing a file based on policy data composed of the path information of the directory and the policy attribute data.

17. A computer-readable storage medium on which is recorded a program for causing a computer to execute a process, said process comprising:

setting policy attribute data indicating a policy on which file management is based, in correspondence with path information of a directory and file usage specified by an administrative user; and

assigning at least one of policy attribute data for files in the directory to be inherited to a subdirectory, and assigning specified policy attribute data for files in the subdirectory to a corresponding subdirectory when moving the directory.

18. A file management method for a file system having at least one volume, comprising:

setting policy attribute data indicating a policy, determined by an administrative user, for storing a file depending on type of information in the file, file usage specified by an administrative user and path information of a directory in which the file is stored; and

managing the file based on policy data composed of the path information of the directory and the policy attribute data.

IX. Evidence Appendix

(None)

X. Related Proceedings Appendix

(None)